# z/OS Open Tools

**Students:** Dian Zhu and Kepler Boyce
**Mentors:** Igor Todorovski

Georgia Tech Open Source Program Office

## Project Overview

The summer project is to implement new features for z/OS open tools (zopen package manager).

The first feature is to implement a vulnerability auditing system for the zopen package manager to build a cache of vulnerabilities and provide vulnerability information to users.

The other feature is to integrate AI LLM into zopen build and then zopen build can talk to LLM about the error. The LLM will assist in debugging the error when zopen build provides error to LLM.

See z/OS open tools resources at https://zosopentools.org/#/

## Goals and Milestones 1

- Write scripts to query OSV.dev API and generate vulnerabilities cache and vulnerabilities docs page.

- Modify zopen build to be able to talk to AI LLM when build errors occur.

## Goals and Milestones 2

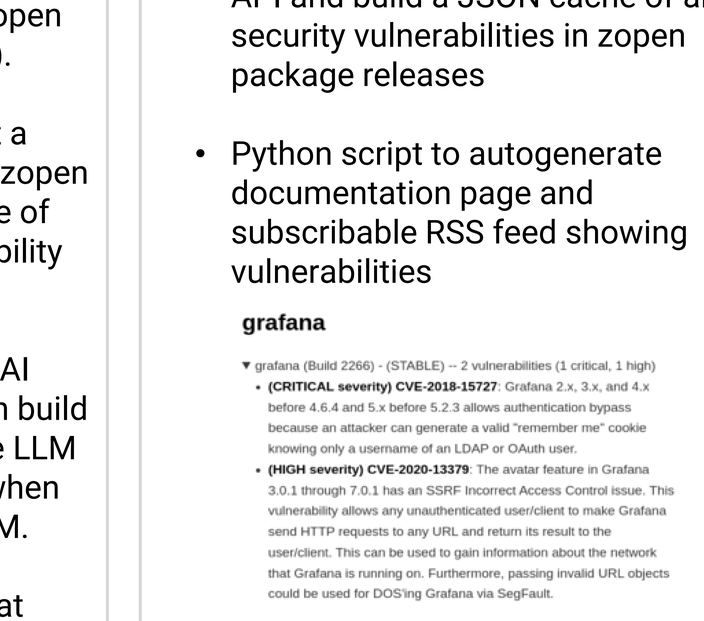
- Add audit command to package manager that reports vulnerability info to users

- Use LLM to give us a solution of the suggested fix if we do zopen build for a project and it fails at a build step.

## Vulnerability Auditing System

- Python script to query OSV.dev API and build a JSON cache of all security vulnerabilities in zopen package releases

- Python script to autogenerate documentation page and subscribable RSS feed showing vulnerabilities

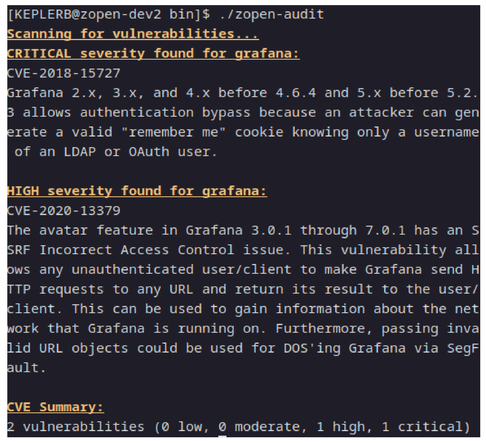


**grafana**

▼ grafana (Build 2266) - (STABLE) -- 2 vulnerabilities (1 critical, 1 high)

- **(CRITICAL severity) CVE-2018-15727**: Grafana 2.x, 3.x, and 4.x before 4.6.4 and 5.x before 5.2.3 allows authentication bypass because an attacker can generate a valid "remember me" cookie knowing only a username of an LDAP or OAuth user.
- **(HIGH severity) CVE-2020-13379**: The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on. Furthermore, passing invalid URL objects could be used for DOS'ing Grafana via SegFault.

- Shell script for zopen audit command that checks JSON cache for any vulnerabilities in installed packages
    - Additional options for removing or attempting to upgrade vulnerable packages



```
[KEPLERB@zopen-dev2 bin]$ ./zopen-audit
Scanning for vulnerabilities...
CRITICAL severity found for grafana:
CVE-2018-15727
Grafana 2.x, 3.x, and 4.x before 4.6.4 and 5.x before 5.2.
3 allows authentication bypass because an attacker can gen
erate a valid "remember me" cookie knowing only a username
 of an LDAP or OAuth user.

HIGH severity found for grafana:
CVE-2020-13379
The avatar feature in Grafana 3.0.1 through 7.0.1 has an S
SRF Incorrect Access Control issue. This vulnerability all
ows any unauthenticated user/client to make Grafana send H
TTP requests to any URL and return its result to the user/
client. This can be used to gain information about the net
work that Grafana is running on. Furthermore, passing inva
lid URL objects could be used for DOS'ing Grafana via SegF
ault.

CVE Summary:
2 vulnerabilities (0 low, 0 moderate, 1 high, 1 critical)
```

## AI LLM Integration

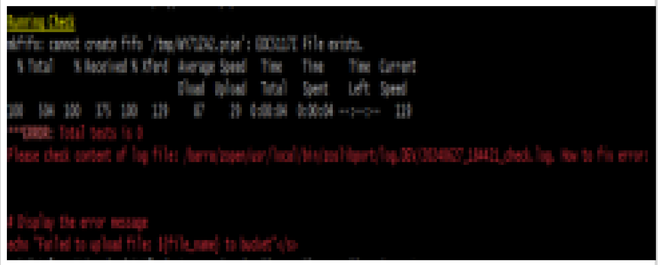
- Set up LocalAI and we get it work with tinyllama model on own desktop first


See LocalAI resources at https://localai.io

- Connect to LocalAI and then run tinyllama model from Z/OS system by sending curl command

- Modify zopen-build file by using Shell code, add curl command containing tinyllama model for error ca se, add new option -- ai to control curl command

- When we do zopen build --ai for a project likes makeport, zopen build --ai will send error to tinyllama model via curl command if build step fails, the model will provide what patch we need to do.



error message and model's response are marked in red

See code at Github here

## Open Source Outcomes

The implementation of vulnerability auditing system provides users vulnerability information in their installed zopen packages, and the integration of AI tinyllama model assists us in finding ways of fixing error of zopen build. These new features impact z/OS development by improving quality of z/OS.

## Future Work

- Check if there exists any issue in z/OS existing tools and improve their quality

- Port new tools to z/OS and contribute the changes to z/OS

Georgia Tech